Ripristino delle applicazioni

Trident

NetApp
February 02, 2026

Sommario

Ripristino delle applicazioni

Ripristina le applicazioni utilizzando Trident Protect

Puoi utilizzare Trident Protect per ripristinare la tua applicazione da uno snapshot o da un backup. Il ripristino da uno snapshot esistente sarà più rapido se si ripristina l'applicazione nello stesso cluster.

- Quando si ripristina un'applicazione, tutti i collegamenti di esecuzione configurati per l'applicazione vengono ripristinati con l'applicazione. Se è presente un gancio di esecuzione post-ripristino, viene eseguito automaticamente come parte dell'operazione di ripristino.
- Il ripristino da un backup a un namespace diverso o al namespace originale è supportato per i volumi qtree. Tuttavia, il ripristino da uno snapshot a un namespace diverso o al namespace originale non è supportato per i volumi qtree.
- È possibile utilizzare le impostazioni avanzate per personalizzare le operazioni di ripristino. Per saperne di più, fare riferimento a "Utilizza le impostazioni di ripristino avanzate Trident Protect".

Ripristino da un backup a uno spazio dei nomi diverso

Quando si ripristina un backup in uno spazio dei nomi diverso utilizzando un CR BackupRestore, Trident Protect ripristina l'applicazione in un nuovo spazio dei nomi e crea un CR dell'applicazione per l'applicazione ripristinata. Per proteggere l'applicazione ripristinata, creare backup o snapshot su richiesta oppure stabilire una pianificazione di protezione.

- Il ripristino di un backup in uno spazio dei nomi diverso con le risorse esistenti non altererà le risorse che condividono i nomi con quelli del backup. Per ripristinare tutte le risorse del backup, eliminare e ricreare lo spazio dei nomi di destinazione o ripristinare il backup in un nuovo spazio dei nomi.
- Quando si utilizza una CR per ripristinare un nuovo namespace, è necessario creare manualmente il namespace di destinazione prima di applicare la CR. Trident Protect crea automaticamente gli spazi dei nomi solo quando si utilizza la CLI.

Prima di iniziare

Assicurati che la scadenza del token di sessione AWS sia sufficiente per qualsiasi operazione di ripristino S3 con esecuzione prolungata. Se il token scade durante l'operazione di ripristino, l'operazione potrebbe non riuscire.

- Per ulteriori informazioni sulla verifica della scadenza corrente del token di sessione, fare riferimento "Documentazione di API AWS" al .
- Per ulteriori informazioni sulle credenziali con le risorse AWS, fare riferimento al "Documentazione di AWS IAM".

Quando si ripristinano i backup utilizzando Kopia come strumento di spostamento dati, è possibile specificare facoltativamente annotazioni nel CR o tramite la CLI per controllare il comportamento dell'archiviazione temporanea utilizzata da Kopia. Fare riferimento al "Documentazione Kopia" per maggiori informazioni sulle opzioni che puoi configurare. Utilizzare il `tridentctl-protect create --help` comando per ulteriori informazioni sulla specifica delle annotazioni con la CLI Trident Protect.

Utilizzare un CR

Fasi

1. Creare il file di risorse personalizzate (CR) e assegnargli un nome `trident-protect-backup-restore-cr.yaml`.
2. Nel file creato, configurare i seguenti attributi:
   - **metadata.name**: (*required*) il nome di questa risorsa personalizzata; scegliere un nome univoco e sensibile per il proprio ambiente.
   - **Spec.appArchivePath**: Il percorso all'interno di AppVault in cui sono memorizzati i contenuti di backup. Per trovare il percorso, utilizzare il seguente comando:

     ```
     kubectl get backups <BACKUP_NAME> -n my-app-namespace -o
     jsonpath='{.status.appArchivePath}'
     ```

   - **Spec.appVaultRef**: (*required*) il nome dell'AppVault in cui sono memorizzati i contenuti di backup.
   - **spec.namespaceMapping**: mappatura dello spazio dei nomi di origine dell'operazione di ripristino allo spazio dei nomi di destinazione. Sostituire `my-source-namespace` e `my-destination-namespace` con le informazioni del proprio ambiente.

     ```
     ---
     apiVersion: protect.trident.netapp.io/v1
     kind: BackupRestore
     metadata:
       name: my-cr-name
       namespace: my-destination-namespace
     spec:
       appArchivePath: my-backup-path
       appVaultRef: appvault-name
       namespaceMapping: [{"source": "my-source-namespace",
     "destination": "my-destination-namespace"}]
     ```

3. (*Optional*) se è necessario selezionare solo determinate risorse dell'applicazione da ripristinare, aggiungere un filtro che includa o escluda risorse contrassegnate con determinate etichette:

   > Trident Protect seleziona automaticamente alcune risorse in base alla loro relazione con le risorse selezionate. Ad esempio, se selezioni una risorsa di richiesta di volume persistente e a questa è associato un pod, Trident Protect ripristinerà anche il pod associato.

   - **ResourceFilter.resourceSelectionCriteria**: (Necessario per il filtraggio) utilizzare `Include` o includere o `Exclude` escludere una risorsa definita in resourceMatchers. Aggiungere i seguenti parametri resourceMatcher per definire le risorse da includere o escludere:
     - **ResourceFilter.resourceMatchers**: Una matrice di oggetti resourceMatcher. Se si definiscono più elementi in questa matrice, questi corrispondono come un'operazione OR e i campi all'interno di ogni elemento (gruppo, tipo, versione) corrispondono come un'operazione

AND.

- **ResourceMatchers[].group**: (*Optional*) Gruppo della risorsa da filtrare.
- **ResourceMatchers[].Kind**: (*Optional*) tipo di risorsa da filtrare.
- **ResourceMatchers[].version**: (*Optional*) versione della risorsa da filtrare.
- **ResourceMatchers[].names**: (*Optional*) nomi nel campo Kubernetes metadata.name della risorsa da filtrare.
- **ResourceMatchers[].namespaces**: (*Optional*) Namespaces nel campo Kubernetes metadata.name della risorsa da filtrare.
- **ResourceMatchers[].labelSelectors**: (*Optional*) stringa del selettore di etichette nel campo Kubernetes metadata.name della risorsa come definito nella "Documentazione Kubernetes" . Ad esempio: `"trident.netapp.io/os=linux"`.

  Ad esempio:

```
spec:
  resourceFilter:
    resourceSelectionCriteria: "Include"
    resourceMatchers:
      - group: my-resource-group-1
        kind: my-resource-kind-1
        version: my-resource-version-1
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
      - group: my-resource-group-2
        kind: my-resource-kind-2
        version: my-resource-version-2
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
```

4. Dopo aver popolato il `trident-protect-backup-restore-cr.yaml` file con i valori corretti, applicare la CR:

```
kubectl apply -f trident-protect-backup-restore-cr.yaml
```

Utilizzare la CLI

Fasi

1. Ripristinare il backup su uno spazio dei nomi diverso, sostituendo i valori tra parentesi con le informazioni provenienti dall'ambiente. L' `namespace-mapping`argomento utilizza spazi dei nomi separati da due punti per mappare gli spazi dei nomi di origine agli spazi dei nomi di destinazione corretti nel formato `source1:dest1,source2:dest2`. Ad esempio:

```
tridentctl-protect create backuprestore <my_restore_name> \
--backup <backup_namespace>/<backup_to_restore> \
--namespace-mapping <source_to_destination_namespace_mapping> \
-n <application_namespace>
```

Eseguire il ripristino da un backup nello spazio dei nomi originale

È possibile ripristinare un backup nello spazio dei nomi originale in qualsiasi momento.

Prima di iniziare

Assicurati che la scadenza del token di sessione AWS sia sufficiente per qualsiasi operazione di ripristino S3 con esecuzione prolungata. Se il token scade durante l'operazione di ripristino, l'operazione potrebbe non riuscire.

- Per ulteriori informazioni sulla verifica della scadenza corrente del token di sessione, fare riferimento "Documentazione di API AWS" al .
- Per ulteriori informazioni sulle credenziali con le risorse AWS, fare riferimento al "Documentazione di AWS IAM".

> Quando si ripristinano i backup utilizzando Kopia come strumento di spostamento dati, è possibile specificare facoltativamente annotazioni nel CR o tramite la CLI per controllare il comportamento dell'archiviazione temporanea utilizzata da Kopia. Fare riferimento al "Documentazione Kopia" per maggiori informazioni sulle opzioni che puoi configurare. Utilizzare il `tridentctl-protect create --help` comando per ulteriori informazioni sulla specifica delle annotazioni con la CLI Trident Protect.

Utilizzare un CR

Fasi

1. Creare il file di risorse personalizzate (CR) e assegnargli un nome `trident-protect-backup-ipr-cr.yaml`.
2. Nel file creato, configurare i seguenti attributi:
   - **metadata.name**: (*required*) il nome di questa risorsa personalizzata; scegliere un nome univoco e sensibile per il proprio ambiente.
   - **Spec.appArchivePath**: Il percorso all'interno di AppVault in cui sono memorizzati i contenuti di backup. Per trovare il percorso, utilizzare il seguente comando:

     ```
     kubectl get backups <BACKUP_NAME> -n my-app-namespace -o jsonpath='{.status.appArchivePath}'
     ```

   - **Spec.appVaultRef**: (*required*) il nome dell'AppVault in cui sono memorizzati i contenuti di backup.

     Ad esempio:

```
---
apiVersion: protect.trident.netapp.io/v1
kind: BackupInplaceRestore
metadata:
  name: my-cr-name
  namespace: my-app-namespace
spec:
  appArchivePath: my-backup-path
  appVaultRef: appvault-name
```

3. (*Optional*) se è necessario selezionare solo determinate risorse dell'applicazione da ripristinare, aggiungere un filtro che includa o escluda risorse contrassegnate con determinate etichette:

   Trident Protect seleziona automaticamente alcune risorse in base alla loro relazione con le risorse selezionate. Ad esempio, se selezioni una risorsa di richiesta di volume persistente e a questa è associato un pod, Trident Protect ripristinerà anche il pod associato.

   - **ResourceFilter.resourceSelectionCriteria**: (Necessario per il filtraggio) utilizzare `Include` o includere o `Exclude` escludere una risorsa definita in resourceMatchers. Aggiungere i seguenti parametri resourceMatcher per definire le risorse da includere o escludere:
     - **ResourceFilter.resourceMatchers**: Una matrice di oggetti resourceMatcher. Se si definiscono più elementi in questa matrice, questi corrispondono come un'operazione OR e i campi all'interno di ogni elemento (gruppo, tipo, versione) corrispondono come un'operazione AND.
       - **ResourceMatchers[].group**: (*Optional*) Gruppo della risorsa da filtrare.
       - **ResourceMatchers[].Kind**: (*Optional*) tipo di risorsa da filtrare.

- **ResourceMatchers[].version**: (*Optional*) versione della risorsa da filtrare.
- **ResourceMatchers[].names**: (*Optional*) nomi nel campo Kubernetes metadata.name della risorsa da filtrare.
- **ResourceMatchers[].namespaces**: (*Optional*) Namespaces nel campo Kubernetes metadata.name della risorsa da filtrare.
- **ResourceMatchers[].labelSelectors**: (*Optional*) stringa del selettore di etichette nel campo Kubernetes metadata.name della risorsa come definito nella "Documentazione Kubernetes" . Ad esempio: `"trident.netapp.io/os=linux"`.

  Ad esempio:

```
spec:
  resourceFilter:
    resourceSelectionCriteria: "Include"
    resourceMatchers:
      - group: my-resource-group-1
        kind: my-resource-kind-1
        version: my-resource-version-1
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
      - group: my-resource-group-2
        kind: my-resource-kind-2
        version: my-resource-version-2
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
```

4. Dopo aver popolato il `trident-protect-backup-ipr-cr.yaml` file con i valori corretti, applicare la CR:

```
kubectl apply -f trident-protect-backup-ipr-cr.yaml
```

Utilizzare la CLI

Fasi

1. Ripristinare il backup nello spazio dei nomi originale, sostituendo i valori tra parentesi con le informazioni provenienti dall'ambiente. L'`backup`argomento utilizza uno spazio dei nomi e un nome di backup nel formato `<namespace>/<name>`. Ad esempio:

```
tridentctl-protect create backupinplacerestore <my_restore_name> \
--backup <namespace/backup_to_restore> \
-n <application_namespace>
```

Ripristino da un backup a un cluster diverso

In caso di problemi con il cluster originale, è possibile ripristinare un backup su un cluster diverso.

- Quando si ripristinano i backup utilizzando Kopia come strumento di spostamento dati, è possibile specificare facoltativamente annotazioni nel CR o tramite la CLI per controllare il comportamento dell'archiviazione temporanea utilizzata da Kopia. Fare riferimento al "Documentazione Kopia" per maggiori informazioni sulle opzioni che puoi configurare. Utilizzare il `tridentctl-protect create --help` comando per ulteriori informazioni sulla specifica delle annotazioni con la CLI Trident Protect.
- Quando si utilizza una CR per ripristinare un nuovo namespace, è necessario creare manualmente il namespace di destinazione prima di applicare la CR. Trident Protect crea automaticamente gli spazi dei nomi solo quando si utilizza la CLI.

Prima di iniziare

Assicurarsi che siano soddisfatti i seguenti prerequisiti:

- Nel cluster di destinazione è installato Trident Protect.
- Il cluster di destinazione ha accesso al percorso bucket dello stesso AppVault del cluster di origine, dove è memorizzato il backup.
- Assicurarsi che l'ambiente locale possa connettersi al bucket di archiviazione degli oggetti definito in AppVault CR durante l'esecuzione di `tridentctl-protect get appvaultcontent` comando. Se le restrizioni di rete impediscono l'accesso, eseguire invece la CLI Trident Protect da un pod sul cluster di destinazione.
- Assicurati che la scadenza del token di sessione AWS sia sufficiente per qualsiasi operazione di ripristino con esecuzione prolungata. Se il token scade durante l'operazione di ripristino, l'operazione potrebbe non riuscire.
  - Per ulteriori informazioni sulla verifica della scadenza corrente del token di sessione, fare riferimento "Documentazione di API AWS" al .
  - Per ulteriori informazioni sulle credenziali con le risorse AWS, fare riferimento al "Documentazione AWS".

Fasi

1. Verificare la disponibilità di AppVault CR sul cluster di destinazione utilizzando il plug-in Trident Protect CLI:

```
tridentctl-protect get appvault --context <destination_cluster_name>
```

Verificare che lo spazio dei nomi destinato al ripristino dell'applicazione esista nel cluster di destinazione.

2. Visualizzare il contenuto di backup dell'AppVault disponibile dal cluster di destinazione:

```
tridentctl-protect get appvaultcontent <appvault_name> \
--show-resources backup \
--show-paths \
--context <destination_cluster_name>
```

L’esecuzione di questo comando visualizza i backup disponibili in AppVault, inclusi i relativi cluster di origine, i nomi delle applicazioni corrispondenti, i timestamp e i percorsi di archivio.

Esempio di output:

```
+-------------+-----------+--------+-----------------
+--------------------------+-------------+
|   CLUSTER   |    APP    |  TYPE  |      NAME       |        TIMESTAMP
|    PATH     |
+-------------+-----------+--------+-----------------
+--------------------------+-------------+
| production1 | wordpress | backup | wordpress-bkup-1| 2024-10-30
08:37:40 (UTC)| backuppath1 |
| production1 | wordpress | backup | wordpress-bkup-2| 2024-10-30
08:37:40 (UTC)| backuppath2 |
+-------------+-----------+--------+-----------------
+--------------------------+-------------+
```

3. Ripristinare l’applicazione nel cluster di destinazione utilizzando il nome AppVault e il percorso di archiviazione:

Utilizzare un CR

1. Creare il file di risorse personalizzate (CR) e assegnargli un nome `trident-protect-backup-restore-cr.yaml`.
2. Nel file creato, configurare i seguenti attributi:
   - **metadata.name**: (*required*) il nome di questa risorsa personalizzata; scegliere un nome univoco e sensibile per il proprio ambiente.
   - **Spec.appVaultRef**: (*required*) il nome dell'AppVault in cui sono memorizzati i contenuti di backup.
   - **Spec.appArchivePath**: Il percorso all'interno di AppVault in cui sono memorizzati i contenuti di backup. Per trovare il percorso, utilizzare il seguente comando:

     ```
     kubectl get backups <BACKUP_NAME> -n my-app-namespace -o
     jsonpath='{.status.appArchivePath}'
     ```

     Se BackupRestore CR non è disponibile, è possibile utilizzare il comando menzionato al passaggio 2 per visualizzare il contenuto del backup.

   - **spec.namespaceMapping**: mappatura dello spazio dei nomi di origine dell'operazione di ripristino allo spazio dei nomi di destinazione. Sostituire `my-source-namespace` e `my-destination-namespace` con le informazioni del proprio ambiente.

     Ad esempio:

```
apiVersion: protect.trident.netapp.io/v1
kind: BackupRestore
metadata:
  name: my-cr-name
  namespace: my-destination-namespace
spec:
  appVaultRef: appvault-name
  appArchivePath: my-backup-path
  namespaceMapping: [{"source": "my-source-namespace", "
destination": "my-destination-namespace"}]
```

3. Dopo aver popolato il `trident-protect-backup-restore-cr.yaml` file con i valori corretti, applicare la CR:

```
kubectl apply -f trident-protect-backup-restore-cr.yaml
```

Utilizzare la CLI

1. Utilizzare il seguente comando per ripristinare l'applicazione, sostituendo i valori tra parentesi con le informazioni dell'ambiente. L'argomento namespace-mapping utilizza spazi dei nomi separati da due punti per mappare gli spazi dei nomi di origine agli spazi dei nomi di destinazione corretti nel formato

source1:dest1,source2:dest2. Ad esempio:

```
tridentctl-protect create backuprestore <restore_name> \
--namespace-mapping <source_to_destination_namespace_mapping> \
--appvault <appvault_name> \
--path <backup_path> \
--context <destination_cluster_name> \
-n <application_namespace>
```

Ripristino da uno snapshot a uno spazio dei nomi diverso

È possibile ripristinare i dati da uno snapshot utilizzando un file di risorse personalizzato (CR) in uno spazio dei nomi diverso o nello spazio dei nomi di origine originale. Quando si ripristina uno snapshot in un namespace diverso utilizzando un CR SnapshotRestore, Trident Protect ripristina l'applicazione in un nuovo namespace e crea un CR per l'applicazione ripristinata. Per proteggere l'applicazione ripristinata, creare backup o snapshot su richiesta oppure stabilire una pianificazione di protezione.

- SnapshotRestore supporta il `spec.storageClassMapping` attributo, ma solo quando le classi di archiviazione di origine e di destinazione utilizzano lo stesso backend di archiviazione. Se si tenta di ripristinare un `StorageClass` che utilizza un backend di archiviazione diverso, l'operazione di ripristino non riuscirà.
- Quando si utilizza una CR per ripristinare un nuovo namespace, è necessario creare manualmente il namespace di destinazione prima di applicare la CR. Trident Protect crea automaticamente gli spazi dei nomi solo quando si utilizza la CLI.

Prima di iniziare

Assicurati che la scadenza del token di sessione AWS sia sufficiente per qualsiasi operazione di ripristino S3 con esecuzione prolungata. Se il token scade durante l'operazione di ripristino, l'operazione potrebbe non riuscire.

- Per ulteriori informazioni sulla verifica della scadenza corrente del token di sessione, fare riferimento "Documentazione di API AWS" al .
- Per ulteriori informazioni sulle credenziali con le risorse AWS, fare riferimento al "Documentazione di AWS IAM".

Utilizzare un CR

Fasi

1. Creare il file di risorse personalizzate (CR) e assegnargli un nome `trident-protect-snapshot-restore-cr.yaml`.
2. Nel file creato, configurare i seguenti attributi:
   - **metadata.name**: (*required*) il nome di questa risorsa personalizzata; scegliere un nome univoco e sensibile per il proprio ambiente.
   - **Spec.appVaultRef**: (*required*) il nome dell'AppVault in cui sono memorizzati i contenuti dello snapshot.
   - **Spec.appArchivePath**: Il percorso all'interno di AppVault in cui sono memorizzati i contenuti dello snapshot. Per trovare il percorso, utilizzare il seguente comando:

     ```
     kubectl get snapshots <SNAPHOT_NAME> -n my-app-namespace -o
     jsonpath='{.status.appArchivePath}'
     ```

   - **spec.namespaceMapping**: mappatura dello spazio dei nomi di origine dell'operazione di ripristino allo spazio dei nomi di destinazione. Sostituire `my-source-namespace` e `my-destination-namespace` con le informazioni del proprio ambiente.

     ```
     ---
     apiVersion: protect.trident.netapp.io/v1
     kind: SnapshotRestore
     metadata:
       name: my-cr-name
       namespace: my-app-namespace
     spec:
       appVaultRef: appvault-name
       appArchivePath: my-snapshot-path
       namespaceMapping: [{"source": "my-source-namespace",
     "destination": "my-destination-namespace"}]
     ```

3. (*Optional*) se è necessario selezionare solo determinate risorse dell'applicazione da ripristinare, aggiungere un filtro che includa o escluda risorse contrassegnate con determinate etichette:

   > Trident Protect seleziona automaticamente alcune risorse in base alla loro relazione con le risorse selezionate. Ad esempio, se selezioni una risorsa di richiesta di volume persistente e a questa è associato un pod, Trident Protect ripristinerà anche il pod associato.

   - **ResourceFilter.resourceSelectionCriteria**: (Necessario per il filtraggio) utilizzare `Include` o includere o `Exclude` escludere una risorsa definita in resourceMatchers. Aggiungere i seguenti parametri resourceMatcher per definire le risorse da includere o escludere:
     - **ResourceFilter.resourceMatchers**: Una matrice di oggetti resourceMatcher. Se si definiscono più elementi in questa matrice, questi corrispondono come un'operazione OR e i

campi all'interno di ogni elemento (gruppo, tipo, versione) corrispondono come un'operazione AND.

- **ResourceMatchers[].group**: (*Optional*) Gruppo della risorsa da filtrare.
- **ResourceMatchers[].Kind**: (*Optional*) tipo di risorsa da filtrare.
- **ResourceMatchers[].version**: (*Optional*) versione della risorsa da filtrare.
- **ResourceMatchers[].names**: (*Optional*) nomi nel campo Kubernetes metadata.name della risorsa da filtrare.
- **ResourceMatchers[].namespaces**: (*Optional*) Namespaces nel campo Kubernetes metadata.name della risorsa da filtrare.
- **ResourceMatchers[].labelSelectors**: (*Optional*) stringa del selettore di etichette nel campo Kubernetes metadata.name della risorsa come definito nella "Documentazione Kubernetes" . Ad esempio: `"trident.netapp.io/os=linux"`.

  Ad esempio:

```
spec:
  resourceFilter:
    resourceSelectionCriteria: "Include"
    resourceMatchers:
      - group: my-resource-group-1
        kind: my-resource-kind-1
        version: my-resource-version-1
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
      - group: my-resource-group-2
        kind: my-resource-kind-2
        version: my-resource-version-2
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
```

4. Dopo aver popolato il `trident-protect-snapshot-restore-cr.yaml` file con i valori corretti, applicare la CR:

```
kubectl apply -f trident-protect-snapshot-restore-cr.yaml
```

Utilizzare la CLI

Fasi

1. Ripristinare lo snapshot in uno spazio dei nomi diverso, sostituendo i valori tra parentesi con le informazioni provenienti dall'ambiente.

   - L'`snapshot`argomento utilizza uno spazio dei nomi e un nome snapshot nel formato `<namespace>/<name>.

- L'`namespace-mapping`argomento utilizza spazi dei nomi separati da due punti per mappare gli spazi dei nomi di origine agli spazi dei nomi di destinazione corretti nel formato `source1:dest1,source2:dest2.

  Ad esempio:

```
tridentctl-protect create snapshotrestore <my_restore_name> \
--snapshot <namespace/snapshot_to_restore> \
--namespace-mapping <source_to_destination_namespace_mapping> \
-n <application_namespace>
```

Ripristinare da uno snapshot allo spazio dei nomi originale

È possibile ripristinare uno snapshot nello spazio dei nomi originale in qualsiasi momento.

Prima di iniziare

Assicurati che la scadenza del token di sessione AWS sia sufficiente per qualsiasi operazione di ripristino S3 con esecuzione prolungata. Se il token scade durante l'operazione di ripristino, l'operazione potrebbe non riuscire.

- Per ulteriori informazioni sulla verifica della scadenza corrente del token di sessione, fare riferimento "Documentazione di API AWS" al .
- Per ulteriori informazioni sulle credenziali con le risorse AWS, fare riferimento al "Documentazione di AWS IAM".

Utilizzare un CR

Fasi

1. Creare il file di risorse personalizzate (CR) e assegnargli un nome `trident-protect-snapshot-ipr-cr.yaml`.
2. Nel file creato, configurare i seguenti attributi:
   - **metadata.name**: (*required*) il nome di questa risorsa personalizzata; scegliere un nome univoco e sensibile per il proprio ambiente.
   - **Spec.appVaultRef**: (*required*) il nome dell'AppVault in cui sono memorizzati i contenuti dello snapshot.
   - **Spec.appArchivePath**: Il percorso all'interno di AppVault in cui sono memorizzati i contenuti dello snapshot. Per trovare il percorso, utilizzare il seguente comando:

     ```
     kubectl get snapshots <SNAPSHOT_NAME> -n my-app-namespace -o jsonpath='{.status.appArchivePath}'
     ```

     ```
     ---
     apiVersion: protect.trident.netapp.io/v1
     kind: SnapshotInplaceRestore
     metadata:
       name: my-cr-name
       namespace: my-app-namespace
     spec:
       appVaultRef: appvault-name
       appArchivePath: my-snapshot-path
     ```

3. (*Optional*) se è necessario selezionare solo determinate risorse dell'applicazione da ripristinare, aggiungere un filtro che includa o escluda risorse contrassegnate con determinate etichette:

   > Trident Protect seleziona automaticamente alcune risorse in base alla loro relazione con le risorse selezionate. Ad esempio, se selezioni una risorsa di richiesta di volume persistente e a questa è associato un pod, Trident Protect ripristinerà anche il pod associato.

   - **ResourceFilter.resourceSelectionCriteria**: (Necessario per il filtraggio) utilizzare `Include` o includere o `Exclude` escludere una risorsa definita in resourceMatchers. Aggiungere i seguenti parametri resourceMatcher per definire le risorse da includere o escludere:
     - **ResourceFilter.resourceMatchers**: Una matrice di oggetti resourceMatcher. Se si definiscono più elementi in questa matrice, questi corrispondono come un'operazione OR e i campi all'interno di ogni elemento (gruppo, tipo, versione) corrispondono come un'operazione AND.
       - **ResourceMatchers[].group**: (*Optional*) Gruppo della risorsa da filtrare.
       - **ResourceMatchers[].Kind**: (*Optional*) tipo di risorsa da filtrare.
       - **ResourceMatchers[].version**: (*Optional*) versione della risorsa da filtrare.

- **ResourceMatchers[].names**: (*Optional*) nomi nel campo Kubernetes metadata.name della risorsa da filtrare.
- **ResourceMatchers[].namespaces**: (*Optional*) Namespaces nel campo Kubernetes metadata.name della risorsa da filtrare.
- **ResourceMatchers[].labelSelectors**: (*Optional*) stringa del selettore di etichette nel campo Kubernetes metadata.name della risorsa come definito nella "Documentazione Kubernetes" . Ad esempio: `"trident.netapp.io/os=linux"`.

  Ad esempio:

```
spec:
  resourceFilter:
    resourceSelectionCriteria: "Include"
    resourceMatchers:
      - group: my-resource-group-1
        kind: my-resource-kind-1
        version: my-resource-version-1
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
      - group: my-resource-group-2
        kind: my-resource-kind-2
        version: my-resource-version-2
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
```

4. Dopo aver popolato il `trident-protect-snapshot-ipr-cr.yaml` file con i valori corretti, applicare la CR:

```
kubectl apply -f trident-protect-snapshot-ipr-cr.yaml
```

Utilizzare la CLI

Fasi

1. Ripristinare lo snapshot nello spazio dei nomi originale, sostituendo i valori tra parentesi con le informazioni provenienti dall'ambiente. Ad esempio:

```
tridentctl-protect create snapshotinplacerestore <my_restore_name> \
--snapshot <namespace/snapshot_to_restore> \
-n <application_namespace>
```

Controllare lo stato di un'operazione di ripristino

È possibile utilizzare la riga di comando per verificare lo stato di un'operazione di ripristino in corso, completata o non riuscita.

Fasi

1. Utilizzare il seguente comando per recuperare lo stato dell'operazione di ripristino, sostituendo i valori nei brackes con le informazioni dall'ambiente in uso:

```
kubectl get backuprestore -n <namespace_name> <my_restore_cr_name> -o
jsonpath='{.status}'
```

Utilizza le impostazioni di ripristino avanzate Trident Protect

È possibile personalizzare le operazioni di ripristino utilizzando impostazioni avanzate quali annotazioni, impostazioni dello spazio dei nomi e opzioni di archiviazione per soddisfare esigenze specifiche.

Annotazioni ed etichette del namespace durante le operazioni di ripristino e failover

Durante le operazioni di ripristino e failover, vengono applicate etichette e annotazioni nel namespace di destinazione in modo che corrispondano alle etichette e alle annotazioni nel namespace di origine. Vengono aggiunte etichette o annotazioni dallo spazio dei nomi di origine che non esistono nello spazio dei nomi di destinazione e le etichette o annotazioni già esistenti vengono sovrascritte per corrispondere al valore dello spazio dei nomi di origine. Le etichette o le annotazioni presenti solo nello spazio dei nomi di destinazione rimangono invariate.

Se si utilizza Red Hat OpenShift, è importante tenere presente il ruolo fondamentale delle annotazioni dello spazio dei nomi negli ambienti OpenShift. Le annotazioni dello spazio dei nomi garantiscono che i pod ripristinati aderiscano alle autorizzazioni appropriate e alle configurazioni di sicurezza definite dai vincoli del contesto di sicurezza (SCC) di OpenShift e possano accedere ai volumi senza problemi di autorizzazione. Per maggiori informazioni, fare riferimento al"Documentazione dei vincoli del contesto di protezione OpenShift" .

Puoi impedire la sovrascrittura delle annotazioni specifiche nel namespace di destinazione impostando la variabile dell'ambiente Kubernetes `RESTORE_SKIP_NAMESPACE_ANNOTATIONS` prima di eseguire l'operazione di ripristino o failover. Ad esempio:

```
helm upgrade trident-protect -n trident-protect netapp-trident-
protect/trident-protect \
  --set-string
restoreSkipNamespaceAnnotations="{<annotation_key_to_skip_1>,<annotation_k
ey_to_skip_2>}" \
  --reuse-values
```

Quando si esegue un'operazione di ripristino o failover, tutte le annotazioni e le etichette dello spazio dei nomi specificate in `restoreSkipNamespaceAnnotations` E `restoreSkipNamespaceLabels` sono esclusi dall'operazione di ripristino o failover. Assicurarsi che queste impostazioni siano configurate durante l'installazione iniziale di Helm. Per saperne di più, fare riferimento a "Configurare le impostazioni aggiuntive del grafico del timone Trident Protect".

Se hai installato l'applicazione sorgente utilizzando Helm con `--create-namespace` bandiera, un trattamento speciale è riservato al `name` etichetta chiave. Durante il processo di ripristino o failover, Trident Protect copia questa etichetta nello spazio dei nomi di destinazione, ma aggiorna il valore al valore dello spazio dei nomi di destinazione se il valore dell'origine corrisponde allo spazio dei nomi di origine. Se questo valore non corrisponde allo spazio dei nomi di origine, viene copiato nello spazio dei nomi di destinazione senza modifiche.

Esempio

Nell'esempio seguente viene presentato uno spazio dei nomi di origine e destinazione, ciascuno con annotazioni ed etichette diverse. È possibile visualizzare lo stato dello spazio dei nomi di destinazione prima e dopo l'operazione e il modo in cui le annotazioni e le etichette vengono combinate o sovrascritte nello spazio dei nomi di destinazione.

Prima dell'operazione di ripristino o failover

La tabella seguente illustra lo stato degli spazi dei nomi di origine e di destinazione di esempio prima dell'operazione di ripristino o failover:

Namespace	Annotazioni	Etichette
Namespace ns-1 (origine)	• annotation.one/key: "updatedvalue" • annotation.two/key: "true"	• ambiente=produzione • conformità=hipaa • name=ns-1
Namespace ns-2 (destinazione)	• annotation.one/key: "true" • annotation.three/key: "false"	• ruolo=database

Dopo l'operazione di ripristino

La tabella seguente illustra lo stato dello spazio dei nomi di destinazione di esempio dopo l'operazione di ripristino o failover. Alcune chiavi sono state aggiunte, altre sono state sovrascritte e l' `name`etichetta è stata aggiornata per corrispondere allo spazio dei nomi di destinazione:

Namespace	Annotazioni	Etichette
Namespace ns-2 (destinazione)	• annotation.one/key: "updatedvalue" • annotation.two/key: "true" • annotation.three/key: "false"	• name=ns-2 • conformità=hipaa • ambiente=produzione • ruolo=database

Campi supportati

Questa sezione descrive i campi aggiuntivi disponibili per le operazioni di ripristino.

Mappatura delle classi di archiviazione

IL `spec.storageClassMapping` L'attributo definisce una mappatura da una classe di archiviazione presente nell'applicazione di origine a una nuova classe di archiviazione nel cluster di destinazione. È possibile utilizzarlo durante la migrazione di applicazioni tra cluster con classi di archiviazione diverse o quando si modifica il backend di archiviazione per le operazioni BackupRestore.

Esempio:

```
storageClassMapping:
  - destination: "destinationStorageClass1"
    source: "sourceStorageClass1"
  - destination: "destinationStorageClass2"
    source: "sourceStorageClass2"
```

Annotazioni supportate

Questa sezione elenca le annotazioni supportate per la configurazione di vari comportamenti nel sistema. Se un'annotazione non viene impostata esplicitamente dall'utente, il sistema utilizzerà il valore predefinito.

Annotazione	Tipo	Descrizione	Valore predefinito
proteggi.trident.netapp.io/data-mover-timeout-sec	stringa	Tempo massimo (in secondi) consentito per l'interruzione dell'operazione di spostamento dei dati.	"300"
protect.trident.netapp.io/kopia-content-cache-size-limit-mb	stringa	Limite massimo di dimensione (in megabyte) per la cache dei contenuti di Kopia.	"1000"
protect.trident.netapp.io/pvc-bind-timeout-sec	stringa	Tempo massimo (in secondi) di attesa affinché i nuovi PersistentVolumeClaim (PVC) creati raggiungano il `Bound` fase prima del fallimento delle operazioni. Si applica a tutti i tipi di ripristino CR (BackupRestore, BackupInplaceRestore, SnapshotRestore, SnapshotInplaceRestore). Utilizzare un valore più alto se il backend di archiviazione o il cluster richiedono spesso più tempo.	"1200" (20 minuti)

Informazioni sul copyright

Informazioni sul marchio commerciale